National Aeronautics and
Space Administration

Headquarters
Washington, DC 20546-0001

DEC 19 2008

Reply to Attn of:

Office of the Chief Information Officer

TO: Distribution

FROM: Senior Agency Information Security Officer

SUBJECT: Agency Organization-Defined Information Technology Security Controls

In accordance with Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, and NIST SP 800-53 (Revision 2), *Recommended Security Controls for Federal Information Systems*, agencies have the flexibility to tailor the security control baselines for those security controls where *organization-defined* parameters are indicated. The attachment to this memorandum documents the current NASA *organization-defined* values for those NIST SP 800-53 (Revision 2) IT security controls for NASA High, Moderate, and Low systems.

Effective immediately, these controls must be implemented with the defined values in all new, revised or otherwise modified NASA IT system security plans at all levels of FIPS-199, *Standards for Security Categorization of Federal Information and Information Systems,* security categorizations. These control values are valid until superseded or rescinded by a memorandum from this office or by an official NASA policy.

If you have questions regarding this memorandum, please direct them to Teresa Fryer at 202-358-2177 or teresa.fryer-1@nasa.gov.

Jerry L. Davis

Attachments

DISTRIBUTION:

Center CIOs:
ARC/Chris Kemp
DFRC/Robert Binkley
GRC/Dr. Sasi Pillay
GSFC/Linda Cureton
HQ/Les Newell
JPL/Jim Rinaldi
JSC/Larry Sweet
KSC/Mike Bolger
LaRC/Cathy Mangum
MSFC/John McDougle (Acting)
SSC/Gay Irby
NSSC/Terry Jackson

Mission Directorate CIOs:
Aeronautics/Phil Milstead (Acting)
Exploration/ Beverly Hamilton
Science/Joe Bredekamp
Space Operations/Dan Hedin (Acting)

Center ITSMs
ARC/Ernest Lopez
DFRC/Larry Johnson
GRC/Don Cannatti
GSFC/Joshua Krage
HQ/Greg Kerr
JPL/Jay Brar
JSC/Ted Dyson
KSC/Henry Yu
LaRC/Kendall Freeman
MSFC/Walter Franklin
SSC/Christine Reynolds
NSSC/James Cluff

NASA Organizational Defined Values for NIST SP 800-53 (Rev 2) Security Controls					
Control	NIST 800-53 Security Control	Value for Low	Value for Moderate	Value for High	Comments
AC-2	Define how often information system (IS) accounts will be reviewed	Semi-Annually	Semi-Annually	Semi-Annually	
AC-2(2)	Define the period of time before temporary and emergency accounts are automatically terminated by the system		30 days	30 days	
AC-2(3)	Define the period of time before inactive accounts are automatically disabled by the system		60 days	30 days	
	The Center CIO may approve a wavier for administrative access before completion of the required training for a period of not more than:		90 days	90 Days	
AC-7	For unsuccessful login attempts, define [before the system is automatically locked]				
	The number of unsuccessful attempts:	5	5	5	5 is FDCC setting
	The time period to be used for the unsuccessful attempts (x attempts within y time period)	5 attempts within 15 minutes	5 attempts within 15 minutes	5 attempts within 15 minutes	5 in 15 min is FDCC setting
	The IS will automatically:				
	Lock the account/node for a defined period of time (OR)	15 minutes	15 minutes	15 minutes	15 min is FDCC setting
	Delays next login prompt according to organization-defined delay algorithm	No delay	No delay	No delay	No delay is FDCC setting
AC-10	The number of concurrent sessions for any user			1	
AC-11	The time period of inactivity before the information system automatically initiates a session lock. [OMB M-06-16 states must be at least 30 minutes for remote and mobile devices]		15 minutes	15 minutes	15 min is FDCC setting
AC-12	The time period of inactivity before the information system automatically terminates a **remote** session (For high systems automatic session termination applies to both local and remote sessions)		15 minutes	15 minutes	
AC-13	The system logs of the activities of users shall be reviewed with respect to the enforcement and usage of information system access controls.	Quarterly	60 days	30 days	
AC-18(2)	The time period the organization scans for unauthorized wireless access points and takes appropriate action if such access points are discovered			Semi-Annually	
AT-2	The time period that all users (including managers and senior executives) are exposed to basic system security awareness materials [must be at least annually]	Annually	Annually	Annually	
AT-3	The time period for re-training of personnel with significant IS security roles and responsibilities	Annually	Annually	Annually	
AU-2	The list of events that generate an audit record (AU-2)	Operating system settings from NIST: http://nvd.nist.gov/fdcc/index.cfm	Operating system settings from NIST: http://nvd.nist.gov/fdcc/index.cfm	Operating system settings from NIST: http://nvd.nist.gov/fdcc/index.cfm	FDCC: Operating system settings from NIST: http://nvd.nist.gov/fdcc/index.cfm
AU-5	The actions to be taken in the event of an audit failure or audit storage capacity being reached [shutdown IS, overwrite oldest audit records, stop generating records]	Overwrite oldest audit records	Overwrite oldest audit records	Overwrite oldest audit records and, if capability exists, generate email notification	

Control	NIST 800-53 Security Control	Value for Low	Value for Moderate	Value for High	Comments
AU-5(1)	The percentage of storage capacity that causes the audit system to automatically generate a warning [i.e., warning generated when this percentage is reached]			80%	FDCC: Operating system specified by default 98%
AU-5(2)	Audit failure events that cause the audit system to automatically generate a real-time alert [i.e., real time alert generated when this audit failure event occurs]			1.Hardware failures and/or errors 2.Software failures and/or errors 3.Audit storage capacity exceeded 4.System backup storage capacity exceeded	
AU-6(2)	Inappropriate or unusual activities with security implications that cause automatic alert of security personnel		1. Blacklist Hit 2. Privilege Escalation	1. Blacklist Hit 2. Privilege Escalation 3. Security policy change	
AU-8(1)	Frequency internal information system clocks are synchronized		Daily	Daily	
AU-11	The time period that audit logs are retained	1 year then: Delete/destroy when no longer needed for administrative, legal, audit or other operational purposes (NPR 1441.1)	1 year then: Delete/destroy when no longer needed for administrative, legal, audit or other operational purposes (NPR 1441.1)	1 year then: Delete/destroy when no longer needed for administrative, legal, audit or other operational purposes (NPR 1441.1)	FDCC: Until overwritten by additional logging or system reinstall.
CA-2	The time period between an assessment of the security controls for the IS [must be at least annually]	Annually	Annually	Annually	
CA-5	Plan of Action and Milestones (POA&M)				
	The time period between updates of a systems plan of action and milestones, documenting planned, implemented, and evaluated remedial actions to correct deficiencies identified in the security control assessment	Monthly	Monthly	Monthly	
	From the time of the identification of the security risk or vulnerability, the Security risk assessment shall be completed within:	10 working days	5 working days	5 working days	
	All identified unmitigated risks shall be entered as items in the system POA&M within:	1 month	1 month	1 month	
	The AO shall review the system POA&M :	Semi-Annually	Monthly	Monthly	
	A risk assessment shall be conducted for each unmitigated deficiency or vulnerability in accordance with NIST SP 800-30 to identify its risk to the system as High, Moderate, or Low within	10 Working days from identification of deficiency or vulnerability	5 Working days from identification of deficiency or vulnerability	5 Working days from identification of deficiency or vulnerability	
	The AO shall be advised of all unmitigated risks designated high within <____> working days from identification of deficiency or vulnerability	10	10	10	
	High risks shall be mitigated or risk-accepted by the AO within:	30 Working days	15 Working days	15 Working days	
	High risks that are unmitigated or not risk-accepted by the AO shall be reported as "POA&M Item Past Due" after:	90 Working days	15 Working days	15 Working days	
	The AO will be advised of all unmitigated risks designated moderate within:	30 Working days	15 Working days	15 Working days	
	Moderate risks that are unmitigated or not risk-accepted by the AO shall be reported as "POA&M Item Past Due" after:	6 months	30 Working days	30 Working days	

Control	NIST 800-53 Security Control	Value for Low	Value for Moderate	Value for High	Comments
	The POA&Ms shall be updated by the first day of the month to meet the monthly Agency and FISMA report requirements	POA&M is updated/current on the first of each month.	POA&M is updated/current on the first of each month.	POA&M is updated/current on the first of each month.	
CA-6	The length of time that a Security Accreditation is valid if there are no significant changes to the IS, the IS facility, etc. [per OMB Circular A-130, this must be at least every three years]	3 years	3 years	3 years	
CM-5	Audit, revalidate and/or update the qualified and authorized personnel list for the individuals that have information system access for the purpose of initiating changes	Annually	Semi-Annually	Quarterly	
CM-6	Validate that the configuration settings are being implemented and maintained by using a combination of Agency vulnerability assessment tools, configuration verification tools, and, if required to assure implementation, inspections	Quarterly	Quarterly	Quarterly	
CM-7	The list of prohibited and/or restricted functions, ports, protocols, and/or services for an IS		IS should be assessed for what functions, ports, and/or services are needed and documented in the SSP; everything else should be disabled. The websites http://www.FreeBSD.org/ports/ and http://www.iana.org/assignments/port-numbers should be used to assist this assessment.	IS should be assessed for what functions, ports, and/or services are needed and documented in the SSP; everything else should be disabled. The websites http://www.FreeBSD.org/ports/ and http://www.iana.org/assignments/port-numbers should be used to assist this assessment.	
CM-7(1)	How often the IS is reviewed to identify and eliminate unnecessary functions, ports, protocols, and/or services			Quarterly	
CP-3	How often contingency roles and responsibility refresher training is needed [must be at least annually]	Annually	Annually	Annually	Added Low
CP-4	Contingency plans will be tested:				
	How often [must be at least annually]	Annually	Annually	Annually	Added Low
	What tests and exercises will be used to perform this testing	Test and exercise in accordance with the requirements and strategy of NITR-2810-15 and ITS-SOP-0040.	Test and exercise in accordance with the requirements and strategy of NITR-2810-15 and ITS-SOP-0040.	Test and exercise in accordance with the requirements and strategy of NITR-2810-15 and ITS-SOP-0040.	
CP-5	How often the contingency plan for the IS will be reviewed [must be at least annually]	Annually	Annually	Annually	
CP-7	The time period before alternative processing sites will be used to perform critical mission/business functions when the primary processing capabilities are unavailable	Dependent on recovery time objects of the system as indicated in the Business Impact Analysis and Contingency Plan	Dependent on recovery time objects of the system as indicated in the Business Impact Analysis and Contingency Plan	Dependent on recovery time objects of the system as indicated in the Business Impact Analysis and Contingency Plan	
CP-8	The time period before alternative communication services will be used to support the IS when the primary communication capabilities are unavailable		Dependent on recovery time objects of the system as indicated in the Business Impact Analysis and Contingency Plan	Dependent on recovery time objects of the system as indicated in the Business Impact Analysis and Contingency Plan	
CP-9	Define how often backups of user-level and system level information will be performed.	Weekly	Daily or option of Weekly with daily incremental	Daily	
CP-9(1)	Define how often backup information will be tested to verify media reliability and information integrity		Quarterly	Quarterly	

Control	NIST 800-53 Security Control	Value for Low	Value for Moderate	Value for High	Comments
IA-2(1)	The NIST 800-63 level of multifactor authentication that is employed by an IS for remote access		Level 4 (PIV card or SecureID) For systems with PII, any waivers to this requirement must be approved by the SAISO.		
IA-2(2)	NIST 800-63 level of multifactor authentication that is employed by an IS for local access. Note: Level 4 must be used for remote access for a high system			Level 3 (Entrust) or Level 4 (RSA SecureID or PIV Card)	
IA-4	The time period of inactivity before a user identifier is automatically disabled	60 days	60 days	30 days	
IA-5	For password-based authentication, the information system will require:				
	Minimum number of characters	12	12	12	12 is FDCC setting
	Password to be changed every XX number of days	60	60	60	60 min is FDCC setting
	Passwords to be remembered for XX uses	24	24	24	24 is FDCC setting
IR-2	The time period between refresher training for personnel in their incident response roles and responsibilities [must be at least annually]	Annually	Annually	Annually	Added Low
IR-3	The incident response capability will be tested:				
	How often [must be at least annually]		Annually	Annually	
	The guidance that will be used to test and/or exercise the incident response capabilities to determine effectiveness		Applicable NASA incident response policies and guidance	Applicable NASA incident response policies and guidance	
MA-6	For maintenance:				
	The key IS components requiring maintenance support and spare parts must be identified		Each program should explicitly identify their key components and list these in the SSP.	Each program should explicitly identify their key components and list these in the SSP.	
	Within what period of time of failure will the key IS components be obtained		72 hours **or** 96 hours if (1) the Moderate categorization is **not** based on availability, (2) if supported by the BIA, **and** (3) is approved by the AO	24 hours **or** 48 hours if (1) the High categorization is **not** based on availability, (2) if supported by the BIA, **and** (3) is approved by the AO	
MP-3	Identify any exemptions to the labeling of media types and hardware components [as long as the equipment remains within a secure environment]			No Exemptions	
MP-5(1)	The method used to transport digital and non-digital media outside of controlled areas		1. FIPS 140-2 complaint encryption for Digital Media, 2. Locked container, e.g. locked briefcase, for non-digital media, 3. Transport by a Custodian/courier approved by the ISO, and 4. Formal Log identifying the media, Custodian, time provided to the custodian, and destination	1. FIPS 140-2 complaint encryption for Digital Media, 2. Locked container, e.g. locked briefcase, for non-digital media, 3. Transport by a Custodian/courier approved by the ISO, and 4. Formal Log identifying the media, Custodian, time provided to the custodian, and destination	
MP-5(2)	The method used to document activities related to the transport of IS media		ISO designated custodian/courier, registered mail, or an authorized delivery service with an accountable tracking system and manifest included in shipment	ISO designated custodian/courier, registered mail, or an authorized delivery service with an accountable tracking system and manifest included in shipment	

Control	NIST 800-53 Security Control	Value for Low	Value for Moderate	Value for High	Comments
PE-2	How often the list of personnel who have authorized access to facilities containing IS (except for those areas within the facility officially designated as publicly accessible) will be reviewed and approved by a designated official [must be at least annually]	Annually	Annually	Annually	
PE-3	Physical Access Control				
	For combination lock access systems, the combination shall be changed at least every:	3 months	3 months	3 months	
	For key locks, positive key control shall be established, key accountability be validated at least every:	6 months	6 months	6 months	
PE-8	How often visitor access records will be reviewed by designated officials	Monthly	Monthly	Weekly	
PL-3	How often the security plan for the IS will be reviewed and revised	Annually	Annually	Annually	
PS-2	How often the risk designation for all positions [established as a screening criteria for individuals filling those positions] will be reviewed and revised	Annually	Annually	Annually	
PS-6	Signed access agreements for individuals requiring access to agency information/information systems (before access) are reviewed/updated [orgn defined frequency]	Annually	Annually	Semi-Annually	Added to the list sent to ITSMs
RA-4	How often the IS Risk Assessment will be updated [assuming no significant changes have occurred to the IS, the facilities where the systems reside, or other conditions that may impact the security or accreditation status of the system]	Annually	Annually	Annually	
RA-5	How often the IS will be searched for vulnerabilities [using appropriate vulnerability scanning tools and techniques]		Monthly	Monthly	
RA-5(2)	How often the list of IS vulnerabilities is updated if no significant vulnerabilities have been identified and reported			Quarterly	
SC-5	List the types of denial of service attacks or reference a source for a current list that the IS is protected against	http://www.us-cert.gov and http://www.cert.org/tech_tips/denial_of_service.html websites	http://www.us-cert.gov and http://www.cert.org/tech_tips/denial_of_service.html websites	http://www.us-cert.gov and http://www.cert.org/tech_tips/denial_of_service.html websites	
SC-10	The length of inactive time before a network disconnects a session [after a period of inactivity]		30 minutes	30 minutes	
SI-2	Flaw Remediation				
	Vendor or NASA designated critical patches shall be applied within	72 Hours	72 Hours	72 Hours	
	Center "snapshot" of patch status shall automatically be provided for update of the Agency ERS and used for build of the Agency monthly Patch reports	Weekly	Weekly	Weekly	
	For non-networked systems with absolutely no physical or logical connection to the network, a manual report in Excel format shall be provided to the cognizant Center security representative	Monthly	Monthly	Monthly	

Control	NIST 800-53 Security Control	Value for Low	Value for Moderate	Value for High	Comments
SI-4(5)	A real-time alert is provided for the following indications of compromise or potential compromise			1. Contact with Blacklist 2. Data Leakage (PII) 3. Failed Logons 4. Hardware problems 5, Possible network intrusions 7. Failed MD5 checksums for field integrity checks (e.g., Tripwire)	
SI-6	The IS verifies correct operation of security functions: (select one or more)				
	[upon system startup and restart] and/or [upon command by user with appropriate privilege] and/or [every (define time period)]			Upon system start and restart; upon command by user with appropriate privilege; and every 24 hours (daily).	
SL-6a	And when anomalies are discovered:				
	[notifies system administrator] and/or [shuts the system down] and/or [restarts the system]			Notifies the system administrator.	
SI-7(1)	How often the IS performs integrity scans to reassess the integrity of software and information			Quarterly	